



LegalTech
PUBLISHING

IN PARTNERSHIP WITH
**ABOVE
THE LAW**

DOCUMENT MANAGEMENT

BUYER'S GUIDE: 2023 EDITION

Comprehensive Document and Email Management Enhanced with Security and Governance

“ Legal professionals spend a considerable amount of time in Microsoft Outlook, where all the functionality of iManage Work 10 is conveniently available.”

Company Name Brand
iManage

Product Name Brand(s)
iManage Work 10, iManage Share, iManage Threat Manager

- Latest Developments and Updates**
- **Access iManage Work 10** for documents and email from Microsoft Teams while maintaining DMS security and version control.
 - Add links to iManage documents directly into Microsoft Teams* conversations.
 - Protect important legal documents from external and internal threats with iManage Threat Manager.

A Comprehensive Document Solution
Law firms and corporate legal departments require more than a basic folder structure to

store documents. They need a comprehensive *information* lifecycle management solution that covers all electronic files and records from inception to disposal. In addition to knowing how to find and search information troves, they need the ability to securely share and collaborate on files with outside users, automate routine workflows, and, most importantly, govern and track sensitive corporate work product.

iManage Work 10 is an intuitive cloud-based document and email management solution that enables users to manage information more productively, collaboratively, and securely. The iManage Cloud architecture also supports a suite of security, risk, and governance applications, such as the **iManage Threat Manager**, which offers continuous protection of sensitive data from internal and external threats.

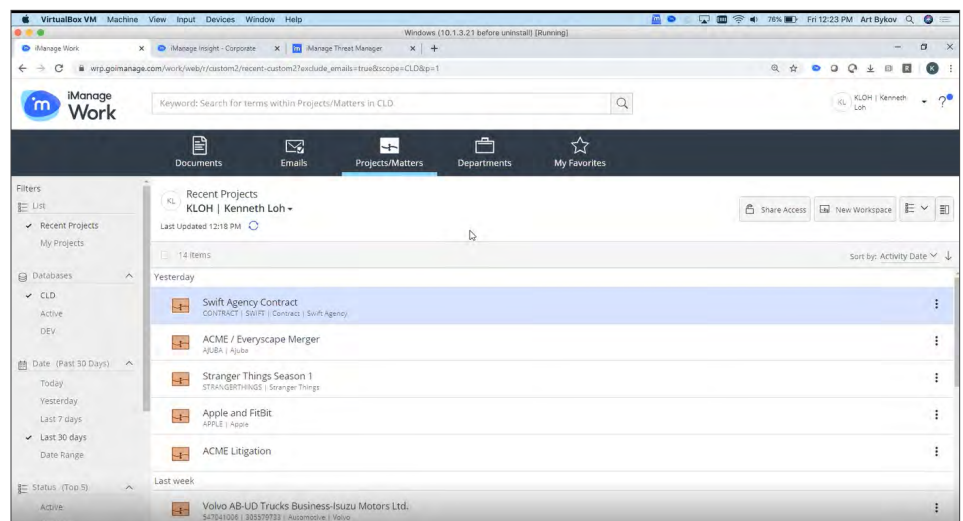


Figure 1: The web-based iManage Work 10 interface offers a list view and a classic grid view for users to pick and choose columns to display. Across the top, various dashboards can be selected to view Documents, Emails, Projects/Matters, Departments, or Favorites. The left panel indicates the available databases or libraries.

*iManage integration with Microsoft Teams is available exclusively to customers on the latest version of iManage Cloud on Azure.

“iManage provides two search options, Personalized and All. The results of a Personalized search lists files you have a prior relationship with.”

Because it's browser-based, everything is available in iManage Work 10 from multiple platforms, including Microsoft Windows, macOS, iOS, and Android. Users can securely access content from anywhere, including their mobile devices, with a consistent experience.

Managing Your Matters

Since most legal teams work from the concept of a “matter” or a “project,” iManage Work 10 delivers a clean, intuitive, browser-based user interface (UI) to support that workflow structure. See *Figure 1 on the previous page*.

Matters contain folders, subfolders, and shared folders (blue, with a people icon) for external collaboration. Each folder has a default document profile that automatically tags filed documents and inherits characteristics from parent folders to facilitate search and maintain security requirements.

iManage Work 10 can easily integrate with matter, practice, and contract management systems to create matching folders. Configurable project and matter templates can generate consistent matter views and set security and sharing parameters. The ability to work from standardized folder structures and templates enables users to intuitively understand where content resides, quickly find what they need, and eliminates the profusion of unstructured folders that plague some systems.

You Work in Outlook? No Problem!
Legal professionals spend a considerable amount of time in Microsoft Outlook, where all the functionality of iManage Work 10 is conveniently available.

Most users set up an extensive array of Outlook folders to store and organize the multitude of messages they send and receive every day, but those folders can't be accessed or searched by other team members. iManage solves this problem by making it easy for users to file a message and attachment to the iManage platform so that it's accessible to others. You simply link an Outlook folder to iManage, then any message you put in that folder can be searched and previewed by others on the team. The iManage Work 10 panel in Outlook can be undocked so you can drag it to a second monitor.

iManage also offers a predictive filing agent that sits atop Outlook. When you select an email, the prediction engine recommends an iManage folder based on your previous filing decisions for similar messages.

Once an email message is filed into an iManage folder, the system displays a green check next to that email in every user's inbox so they don't waste time trying to file duplicate emails. That is all designed to save busy professionals time and mouse clicks, which is one reason iManage is so widely used among legal departments and law firms.

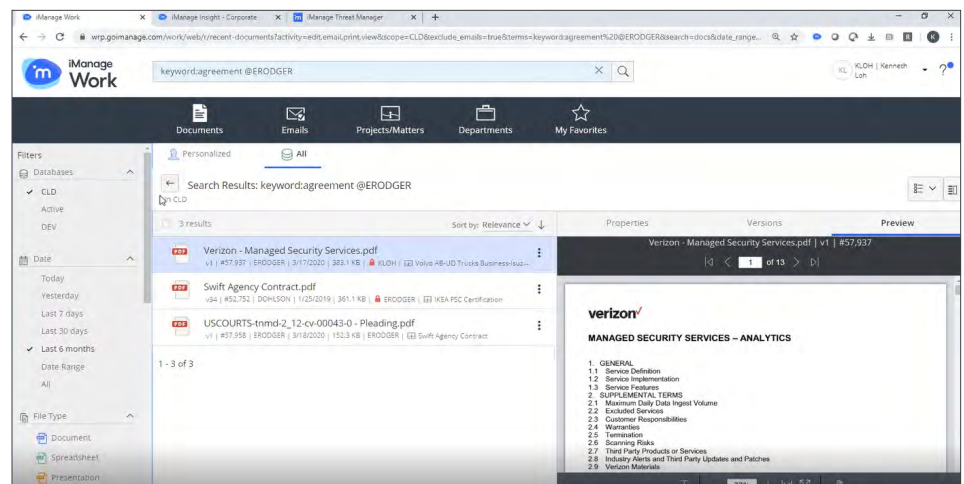


Figure 2: The iManage Work 10 search interface does not require a complex query to find content. Type keywords and use the available filters in the left panel to narrow results and preview documents or email messages. The same search functionality is available in the Outlook panel.

“ iManage Share allows you to create shared folders to easily collaborate on documents with the finance department, human resources, or even outside counsel to assure those files are following your organization’s data governance and security policies.”

File > Save

If you’ve created a new document in Microsoft Word, you can save it directly into iManage with the File > Save command. Instead of tortuously and manually navigating multiple levels of folders and subfolders, the iManage dialog box allows you to profile a document with pertinent information, such as the relevant matter and version number.

Searching the Single Source of Truth

Search becomes most valuable when all of a company’s documents and emails are in a central location—a single source of truth. If you’ve searched Amazon or Google, you’ll be familiar with the general layout of the search window in iManage Work 10. PDF images stored in iManage are automatically scanned with optical character recognition (OCR) technology to search the full text.

iManage’s search window is rooted in the context of the Work 10 dashboard and folder structure. Where you are in the system is where you search. Search parameters support full Boolean logic and proximity searching. The system provides two search options, Personalized and All. The results of a Personalized search lists files you have a prior relationship with, such as matters and files you reviewed or edited in the past.

To expand a search, switch to the All list to narrow the results with filters in the left panel. Various filters are available

depending on the files you’re viewing. For example, for documents, you can choose to see “all latest files,” “last 7 days,” etc. Or, for email, you’ll see filters such as “top senders.” See Figure 2 on the previous page.

Share and Share Alike

Due to the sensitive and often confidential information handled by legal professionals, not all iManage users need access to all matters. But you can securely share documents, even with third parties, using iManage Share, which is included with iManage Work in most Cloud bundles. That allows you to create shared folders to easily collaborate on documents with the finance department, human resources, or even outside counsel to assure those files are following your organization’s data governance and security policies.

iManage Share folders are created with a single mouse click and appear as blue folders inside existing iManage Work 10 projects. Publishing content to those branded cloud folders is a simple drag-and-drop action.

When you attempt to attach a large file to a message in Outlook, iManage Share will suggest sending a secure sharing link instead to reduce the load on your email infrastructure. Your recipient receives a URL they can click to view the secured document. Using the shared link is safer than sending the file as an email attachment because iManage Share is auditable, trackable, and secure. See Figure 3.

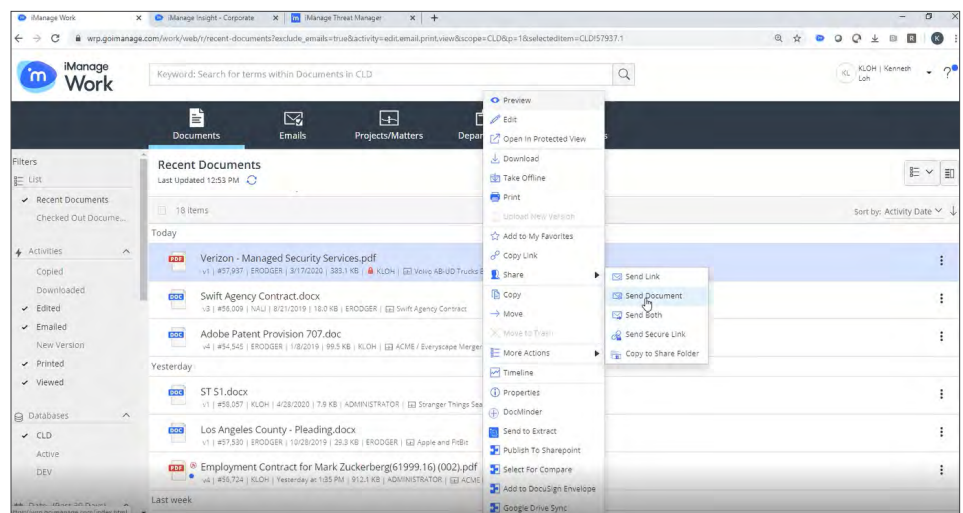


Figure 3: In iManage Work 10, right-click on a document to email the file or share it using a link. To secure content, administrators can disable right-click functions to force users to share a link instead of sending an insecure attachment.

Who is Posing a Threat?

More and more today, legal professionals are getting pulled into discussions about cyber risk. Modern security threats come increasingly from hackers impersonating employees after stealing their login credentials. That's one reason every document stored in iManage has a history timeline from creation to disposition which supports the necessary security audits.

Anytime someone edits, views, or prints a document, that activity is recorded and added to the history. iManage Threat Manager uses those document histories to build a digital fingerprint of each user, and it can use that to help proactively identify active threats or even internal bad actors. It knows, for example, when someone is downloading an unusual volume of content. It also knows when someone who works in IP or Litigation is suddenly looking at content in M&A that is outside the normal behavior for that user. In that way, information stored in iManage becomes some of the best-protected information in the enterprise.

Pricing

iManage offers tailored solution packages to meet the specific needs of customers. The core Work and Share products are

packaged with additional security products in Essentials, Professional, and Enterprise editions. iManage solutions are sold in a Software-as-a-Service (SaaS) subscription pricing model.

Who is iManage?

Founded in 1995, iManage delivers cloud-based services spanning document and email management, collaboration, security, and governance for leading law firms and corporate law departments worldwide. After several mergers and acquisitions, in 2015 the iManage leadership executed a management buyout from HP and the company settled into its headquarters in Chicago, Illinois, with approximately 150 employees. Today, iManage has grown to over 900 employees who support more than 2,500 of the largest law firms and more than 1,400 corporate enterprise and legal customers including more than thirty-seven percent of Fortune 100 organizations and seventy-eight percent of Global 100 Law Firms.

Why Should You Consider iManage?

- Manage content and email communications to improve business processes such as contracts and claims in cloud-based matter files.

- Work efficiently outside the business unit with online collaborative workspaces to share content with corporate departments, outside counsel, and legal service providers.
- Apply information governance and security to critical work product without burdening busy legal professionals.
- Use powerful and personalized search to find previous work products, locate expertise, and gain insight into stored documents and email.

Contact iManage Today!

It's essential to evaluate the capabilities and functionality offered by document management vendors and ensure they align with your legal professionals' specific requirements. Visit the iManage solutions pages to learn more.

- [Corporate Legal Departments](#)
- [Law Firms](#)

Don't Be Caught Unprepared: Secure Your Data Against External and Internal Threats

By: Manuel Sanchez, Information Security & Compliance Specialist at iManage



Manuel Sanchez is an Information Security & Compliance Specialist at iManage with extensive professional experience in information security, governance, and compliance.

The days are long gone when sufficient cybersecurity meant simply installing firewalls and antivirus software. Cybercrime is on the rise, and [experts](#) estimate that the annual costs associated with it will reach \$10.5 trillion worldwide by 2025. Organizations of all kinds are at risk for cyberattacks and should proceed accordingly to protect their sensitive information.

However, cybercriminals are only the start, as not every data security risk your organization faces will come from outsiders.

Information security can be complex and overwhelming, especially in today's rapidly evolving threat landscape. The best protection against security risks is understanding how every employee has a role to play in protecting information assets. Read on to learn more about the ways your organization could be at risk and the best practices you should adopt to secure your data.

Internal Negligence Can Threaten Your Data Security

Contrary to popular belief, most insider threats to organizational data are not bitter former (or soon-to-be-former) employees, but rather well-meaning staff who put data at risk through mistakes or negligence. The [2022 Cost of Insider Threats Global Report](#) found that negligent employees were the root cause of 56% of cybersecurity incidents experienced by survey respondents. Human error, not malicious intent, was responsible for the majority of insider incidents covered in the report.

A good employee education program is key to reducing mistakes that could lead to data breaches. Security awareness training that is both engaging and relevant can help to expose common mistakes and allow employees to adapt security best practices into their working routines.

Employee Turnover Can Compromise Your Information

Soon-to-be former employees pose their own set of risks. Between the ongoing resignation trend and layoffs associated with current economic uncertainty, it's safe to say that employee churn is still high. This is more than a staffing and resource issue—it can also affect the security of your information. When employees leave, they may want to take your information with them. According to [recent data](#), 53% of employees believe that because they worked on a document, it belongs to them. So, malicious or not, employees who leave may exit with confidential documents in (virtual) hand.

To combat this risk, organizations need to ensure that their internal policies cover the rules around company data and that these are clearly understood by all employees. Being fully aware that they are in breach of company policies should deter employees serving their notice from taking documents with them in most cases.

Remote Working Can Bring New Risks to Your Organization

Remote and hybrid work are here to stay. According to data from the [Pew Research Center](#), before the onset of COVID-19, approximately 23% of individuals who were able to do their jobs remotely worked from home all or most of the time. In early 2022, that number had grown dramatically to 59%.

Although remote and hybrid working offer numerous advantages, they also bring risk. Many cybercriminals are targeting remote workers since home networks and personal devices are typically not as fully protected as ones in the office. Criminals also expect remote workers to have their guard down at home and take advantage of this by targeting remote employees with social engineering attacks like phishing.

Ensure remote workers complete security awareness training that will teach them to keep their guard up and avoid falling victim to the social engineering techniques used by bad actors to gain access to user credentials.

Remaining On-Premises Can Limit Threat Readiness

Not every legal organization has its own dedicated IT team. When they do have dedicated IT support, they are often focused on the routine maintenance of on-premises technology. Organizations of all kinds are constantly under threat, with the average seeing **497 cyberattacks every week**. Software patching is one part of cybersecurity hygiene that helps reduce an organization's attack surface, but manually installing and distributing these updates is a big job for a small IT team.

Moving your document management to the cloud improves security while limiting the IT burden. With cloud solutions, most vendors offer unlimited updates throughout the license period. This eliminates the need for manual patching and ensures your technology always has the latest security updates.

Mitigate Risk in The Cloud

The greater security offered in the cloud goes beyond automatic patching. **Contrary to what some believe**, document management in the cloud is far safer than on-premises.

Modern enterprise cloud is fortified with such an array of cutting-edge defense mechanisms and incorporates such deep, layered security best practices that one of the most common reasons legal organizations share for their decision to migrate their data to the cloud is to reduce their risk exposure.

With infrastructures monitored 24/7/365 by expert, dedicated security teams, best-of-breed network and security tools as standard, and a battalion of sophisticated algorithms continuously examining and guarding data at every layer, no on-premises server network can offer the same degree of protection. Even if they could, the cost would be astronomical.

Furthermore, good cloud technology is built using Zero Trust architecture. Zero Trust is exactly as it sounds: security based on the need to verify every interaction – and nothing that isn't verified can be trusted. An individual's ability to access specific data, move around within the system, and view or modify data with differing permission levels relies on the ability of Zero Trust security checkpoints to validate that the specific user and the device they are using have the appropriate credentials to proceed.

A Unified Approach to Security

Breaches happen for many reasons, including gaps in security infrastructure,

willful or accidental actions by individuals, and incursions by external bad actors. Although migration to the cloud is an important step toward safeguarding your data, ultimately, your organization must develop **a culture of security** to benefit from the move fully. After all, people, both intentionally and unintentionally, are the weakest link of any security system. Clear protocols and good training paired with **the right cloud technology** are your best bet for keeping your organization's data safe.

About iManage

iManage is the company dedicated to Making Knowledge Work™. Its intelligent, cloud-enabled, secure knowledge work platform allows organizations to uncover and activate the knowledge that exists inside their business content and communications. Advanced artificial intelligence and powerful document and email management create connections across data, systems, and people while leveraging the context of organizational content to fuel deep insights, informed business decisions, and collaboration. Underpinned by best-of-breed security and sophisticated workflows and governance approaches, iManage has earned its place as the industry standard by continually innovating to solve complex professional challenges and enabling better business outcomes for over one million professionals across 65+ countries. ■

Thank you for reading, let's keep in touch!

We appreciate the time you spent researching solutions for your law firm. New products, feature updates, and announcements happen throughout the year. So, to help you stay informed we have expanded Legal Tech Publishing's Buyer's Guide Series to include an eBook for nearly every product category. Subscribe to receive notifications when a new guide is released. Follow us on the channels below for updates and special virtual events.



Subscribe to our Vimeo Channel



Follow us on Twitter



Like us on Facebook



Follow us on LinkedIn



This buyer's guide is supported by vendor sponsorships. The products and services selected for the guide are done at the author's discretion. Reviews are also written to reflect the opinion of the author. Each product or service must first be selected for the guide, then invited for inclusion before sponsorship is requested. Additionally, emerging technologies who do not have funding to pay for sponsorship are included based on the level of value they offer to law firms. All sponsorship proceeds go towards the costs associated with the production and distribution of the guide.

legaltechpublishing.com